Atomic Energy Control Board
P.O. Box 1046
Ottawa, Canada
K1P 5S9

Commission de contrôle de l'énergie atomique
C.P. 1046
Ottawa, Canada
K1P 5S9

INFO-0079

NUCLEAR PLANT LICENSING IN CANADA

by

D.J. Whelan

Atomic Energy Control Board
Ottawa, Canada

Presented at
"The CANDU Nuclear Power System"
Technical Seminar in
Jakarta, Indonesia

PRESENTATION

January 1981

NUCLEAR PLANT LICENSING IN CANADA

by

D. J. Whelan
Atomic Energy Control Board

Background

Canada is a federal country composed of 10 Provinces and 2 Territories. In 1946, the federal government created the Atomic Energy Control Act declaring atomic energy as a matter of national interest and establishing the Atomic Energy Control Board (AECB) as the regulatory body for atomic energy. Under the provisions of the Act the AECB is authorized to make regulations on a number of topics including the safety of nuclear plants and heavy water plants.

The requirements for the safety of nuclear plants are addressed in three types of documents.

1. Atomic Energy Control Regulations. These give the fundamental requirements such as maximum permissible doses for the public and for atomic radiation workers. They specify that a licence from the AECB is required for the construction or operation of a nuclear plant. The regulations also authorize the AECB to attach any conditions they deem necessary to such licences.

2. Licence Conditions. By means of conditions attached to a licence the AECB imposes requirements on the licensees. Some of these are standard conditions such as the requirement to make specific reports to the AECB, while others are restrictions applying to specific plants. A copy of an Operating Licence is included in the exhibit.

3. Regulatory Documents. The AECB issues documents describing licensing procedures and safety criteria. These documents are regarded as guides to obtaining a licence and compliance with them is not legally mandatory.

The AECB has the ultimate regulatory responsibility for nuclear plants. However, there are other jurisdictions, both federal and provincial, which are involved in the areas of environment, health, and industrial safety. The AECB cooperates with these jurisdictions to avoid duplication of effort. For example, provincial authorities regulate the certification, fabrication, and inspection of pressure-retaining components and act jointly with the AECB in other areas such as code interpretations and auditing of quality assurance.

..../2

Other than the Atomic Energy Control Act, the only other legislation enacted by Parliament in respect of atomic energy is the Nuclear Liability Act. This Act, which entered into force in October, 1976, places total responsibility for nuclear damage on the operator of a nuclear installation. It requires the operator to obtain insurance in the amount of $75 million. It also provides for the establishment of a Nuclear Damage Claims Commission to deal with claims for compensation when the federal government deems that a special tribunal is necessary. The Act recognizes that Canada may enter into international arrangements in respect of nuclear liability but Canada is not at present a party to any such arrangement.

Historical

The safety philosophy which evolved in Canada started with the simple premise that the risk from a nuclear plant must be acceptably small. Risk is defined as the frequency of an event multiplied by its consequences. Consequences are measured in terms of radiation dose to members of the public.

If a nuclear plant had no special safety systems to mitigate the consequences of mishaps, the risk would be entirely unacceptable. This is because the frequency of events which could cause a significant release of radioactive material to the public could be about once in three years. A nuclear plant was visualized therefore as consisting of process systems and safety systems. The process systems consisted of all the equipment needed for the normal operation of the plant and for the routine industrial protection of operators and equipment. Safety systems were additional defences to protect the public from radiation doses arising from failures in the process systems.

In the early 1960's this concept was developed by Dr. G. C. Laurence, president of the AECB, to the point where definitive design principles were adopted. Process systems were to have a high degree of reliability so that failures were minimized. A serious process failure is one which, in the absence of special safety system action, could lead to a dose to the public in excess of a specified limit. Designers were expected to design all process systems to keep the frequency of serious process failures as low as reasonably achievable. Even with this quality of design it was expected that the frequency of serious process failures would be about one in three years.

An important parameter for a safety system is its unavailability, i.e. the time fraction during which the system is unable to perform at its specified effectiveness. This unavailability was specified to be less than $10^{-2.5}$ i.e. the system should not be less effective than specified for more than one day per year.

..../3

Dose limits for individuals and for the population around the plant site were specified for any serious process failure and for any dual failure, (i.e. a serious process failure and unavailability of a special safety system). The meteorology during such accident conditions was also specified.

It followed directly from this approach that the safety systems should be independent from the process systems and from each other to the greatest extent practicable. Furthermore, the specified unavailability of the safety systems was set at a value which could be demonstrated in operation, and it was required that each safety system be readily testable.

This rather simple set of rules was the basis on which designers could determine design rules, and codes and standards for the process and safety systems. The approach deliberately avoided the imposition of detailed design requirements and left the designers free to exercise their ingenuity to optimize the design so as to meet the basic safety criteria. The approach clearly assigned to the owner of the plant the prime responsibility for ensuring a high degree of safety.

The first major change to these criteria occurred in 1972 when the number of safety systems was increased to incorporate a second shutdown system. This relieved the owner of the requirement to analyze each serious process failure with a failure to shut down, i.e. it was accepted that at least one of the shutdown systems would operate as designed when shutdown action was required. However, it had to be shown that the combined action of both shutdown systems was not required to limit the consequences of single and dual failures to acceptable values. Furthermore, the specified unavailability of each safety system was reduced to 10^{-3}.

This approach continued to require that a matrix of accidents be analyzed identifying the consequences of single and dual failures and the reference dose limits for these accidents is shown in Table 1.

TABLE 1

OPERATING DOSE LIMITS AND REFERENCE DOSE LIMITS FOR ACCIDENT CONDITIONS

Situation	Assumed Maximum Frequency	Meteorology to be Used in Calculation	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Normal Operation		Weighted according to effect, i.e. frequency times dose for unit release	0.5 rem/yr whole body 3 rem/yr to thyroid[a]	10^4 man-rem/yr 10^4 thyroid rem/yr
Serious Process Equipment Failure	1 per 3 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete		
Process Equipment Failure plus Failure of any Safety System	1 per 3×10^3 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	25 rem whole body 250 rem thyroid[b]	10^4 man-rem 10^4 thyroid-rem

[a] For other organs use 1/10 ICRP occupational values

[b] For other orgins use 5 times ICRP annual occupational dose (tentative)

..../4

This, in effect, demonstrated the effectiveness of the safety systems. However, this process did not deal explicitly with the following areas of concern.

1. Dual Process System Failures: It was recognized that some of the process systems (e.g. Class III electrical power) had a protective function. Failure of the normal Class IV power combined with failure of the Class III standby generators would eventually have serious consequences for the plant.

2. Failure of Safety Support Systems: Some systems, e.g. instrument air, service water, Class I, II and III electrical power are needed to support process systems and the long term actions of safety systems. Failure of such a system could, in the long term, cause a common-mode failure of a process system and safety system.

3. Post-Accident Phase: In some situations this phase could be about 12 months. It is necessary, therefore, to consider random failures of process systems and the occurrence of earthquakes during this period. Also, the analyses must consider more realistic meteorological conditions than is appropriate during the short term of the initiating accident.

4. Common-Mode Events: It is necessary to design for and analyze the consequences of natural and man-made events which could damage both process and safety systems. Examples are earthquakes, missiles from turbines and aircraft, and fires.

For all of these events the safety systems must be effective to limit the short term consequences. In the longer term it must be shown that the reactor can be kept shut down, its decay heat removed, and its safety status monitored. To ensure a high reliability for these three safety functions designers have arranged the required safety-related systems into two independent and physically separated groups. Group One includes most of the process systems, Class III standby generators and electrical system, shutdown system No. 1, and emergency core cooling system. Group Two includes shutdown system No. 2, the containment system, the emergency power generators and electrical system, and the emergency water system.

The analysis of events with long-term implications for plant safety is performed by a technique known as a Safety Design Matrix. This consists of two sections known as the fault tree and the event tree. The fault tree identifies all the mechanisms which can lead to a fault such as failure of instrument air. The event tree identifies the resulting mechanisms by which radioactive material could escape to the environment and demonstrates the defences for each mechanism. This technique proves that the defences are truly independent of the fault and demonstrates that the three safety functions are maintained with a high degree of confidence.

..../5

This technique has been highly successful in identifying to the designer requirements such as redundancy and separation within safety-related systems. It is also an excellent method of identifying operator actions required following a fault or accident.

So far I have talked only about dose limits for accident situations. The dose limits specified for normal operation correspond to those recommended by the International Commission for Radiological Protection (ICRP). However, the Commission recommended that the actual doses be maintained as low as is reasonably achievable. In recognition of this principle, dose targets were set at 1% of the specific limits.

Present Situation

The present situation is that the reference dose limits in Table 1 must be met for the matrix of single and dual accidents. Also multiple process failures, failures of safety support systems, and natural and man-made internal and external events must be considered and shown to be acceptable. A detailed list of safety requirements is given in Appendix 1.

These are the fundamental principles. From these are derived the specific rules, procedures and practices relating to design, construction, commissioning and operation, and the review and quality assurance procedures to show compliance with the various rules.

It is still the intention to avoid over-regulation which impedes the ingenuity of the designer and may be counter productive in terms of safety. However, as the nuclear industry in Canada has grown it has been necessary to document in greater detail some of the various rules and practices.

There are three different mechanisms by which acceptable design requirements may be established.

1. The designers may document their design intent and submit them to the AECB for approval, e.g. design guides on seismic philosophy and separation of safety-related systems.

2. The owner may agree to conform to existing codes and standards, e.g.: ASME, IEEE, CNA, which are acceptable to the AECB.

3. The AECB may issue licensing guides which explain their requirements.

..../6

The licensing procedures used in Canada are documented in AECB 1139*. Formal licences are required for construction and operation, but site approval is only a practical administrative step. The site approval stage is used to satisfy the AECB about the suitability of the site from the points of view of land use, population density, seismology, geology, water usage, the hazard from man-made and natural events. This stage is used to inform the public as to the environmental and sociological impact of the plant, and also to satisfy other provincial and federal agencies responsible for environmental concerns.

The major document submitted in an application for a Construction Licence is the Preliminary Safety Report. This is a collation of siting and environmental data, design and procedural considerations, process and safety system descriptions, performance specifications, and scoping analyses which give confidence that the plant will be able to meet all the safety requirements.

The Preliminary Safety Report is updated every year during construction to reflect the evolution of design and safety assessments. When applying for an Operating Licence, the owner submits the Final Safety Report which refects the as-built plant. During the licensing process the owner must develop and implement many procedures and programs which include quality assurance program, test and inspection procedures, in-service inspection program, emergency procedures and staff training program. The AECB assigns project officers to review the design and analytical information and to monitor the commissioning and operation of the plant at site.

The key operating personnel must complete a theoretical and practical training program and pass a rigorous set of AECB examinations before they are licensed to operate the plant.

Comparison With Other Countries

The safety criteria developed by different countries range from being very general, as in the United Kingdom, to being very specific, as in the United States. The criteria developed in Canada lie somewhere in the middle of these two approaches. The intention is to provide guidance to the designer and operator but leave them sufficient flexibility to develop the optimum way of meeting the basic safety requirements.

..../7

* This document, along with four draft licensing guides on special safety systems and accident analysis, is included in the exhibit.

The Canadian criteria have evolved in step with the evolution of the CANDU design, and have been developed with CANDU plants in mind. Similar remarks apply to the criteria of other countries. For example, light water reactor designs would not meet Canadian criteria for many reasons. It would be virtually impossible to have the required physical independence between shut off rods used in the shutdown system and those in the regulatory system. For other reasons, a CANDU plant might not meet criteria which had been developed with light water reactors in mind.

In general, the Canadian approach highlights the availability of a safety function and may specify two completely independent systems to achieve that function. The practice in some other countries is to aim for a high degree of reliability within one system by having a high degree of separation within the redundant parts of the system. For example, the CANDU Class III power system fed by the standby generators would not meet U.S. requirements for the separation between the odd and even components. However, in Canada, the system is backed by a completely independent, physically separated emergency power system which does not have a counterpart in the U.S. practice. Similar comments could be made about the design of shutdown systems.

Many countries follow the U.S. practice of having very specific regulations regarding design requirements, contents of Safety Reports, and analytical techniques. The Canadian approach is to made the regulations more general but authorize the AECB to enforce its requirements by applying conditions to the licences it issues. This approach achieves a satisfactory enforcement of requirements but leaves a significant flexibility to cope with evolving licensing situations.

The content of the formal safety submissions required by the AECB is not as extensive as that required by some other countries. It must be remembered, however, that there are AECB project officers located at the plant sites and at the AECL design office. These officers monitor the design, construction, commissioning and operation functions and have access to all the relevant documentation. This on-going review complements the review of the documents submitted at the formal licensing stages.

In general, the formal licensing submissions regarding design and operation are summary documents and do not go into great detail. Documents such as Design Manuals and Operating Manuals describe the detailed methods used to meet the basic requirements. These latter documents support the formal licensing submissions but can be amended with less formality.

..../8

This approach allows the plant owner some design and operating flexibility in areas which do not have a major impact on safety. To implement this approach it is necessary that all parties have a thorough understanding of the safety requirements and their applications. AECB project officers need a thorough knowledge of the plant and the safety assessments. We believe that this is a good approach and is preferable to blindly following a check list or review plan.

To summarize, the Canadian approach ensures that basic safety requirements are met while allowing flexibility to deal with changing conditions. Over-regulation can detract from safety and unnecessarily restrict production. We believe that our approach can achieve a high degree of safety and still allow the flexibility required to prevent unnecessary interference with plant production.

It is recognized that this process requires the use of well-informed and trained personnel. The AECB is prepared to cooperate with overseas regulatory agencies in explaining their safety criteria and review techniques. This cooperation can take the form of correspondence, periodic meetings, staff attachments and training programs to ensure that overseas regulatory personnel can acquire the knowledge and expertise to make good licensing decisions in their own country.

In conclusion we believe that we have a good process in Canada which we could recommend for use in other countries.

APPENDIX 1

Detailed Safety Requirements

1. Design and construction of components, systems and structures essential to or associated with the reactor shall follow the best applicable code, standard, or practice.

2. The design, quality, and operation of all process systems essential to the reactor shall be such that the total of all serious process failures shall not exceed 1 per 3 years. A serious process failure is one that in the absence of safety system action could lead to a dose to the public in excess of the specified limit.

3. Special safety systems shall by physically and functionally separate from the process systems and from each other to the greatest extent practicable.

4. Each special safety system shall be readily testable, as a system, and shall be tested at a frequency to demonstrate that its unavailability is less than 10^{-3}.

5. The plant shall be designed and operated so that the doses to the public resulting from normal operation are expected to be less than a target value of 1% of the maximum permissible dose limit.

6. The effectiveness of the special safety systems shall be such that the dose to any member of the public resulting from a serious process failure does not exceed 0.5 rem whole body or 3 rem to the thyroid, and the dose to the population around the reactor site shall not exceed 10^4 man-rem or 10^4 thyroid-rem.

7. For any postulated combination of a process failure and failure or unavailability of a pertinent safety system the predicted dose to any individual shall not exceed 25 rem whole body and 250 rem to the thyroid. The corresponding dose to the population shall not exceed 10^6 man-rem or 10^6 thyroid-rem.

8. There shall be two shutdown systems which are of diverse design, and physically and functionally independent of each other.

..../2

9. Each shutdown system shall incorporate sufficient redundancy to ensure that no single failure results in the loss of its protective action.

10. Where practicable, two diverse trip parameters shall be incorporated into the sensing and control logic of each shutdown system for every serious process failure.

11. The combined action of the two shutdown systems shall not be required to prevent the consequences of a failure from exceeding the limits specified earlier.

12. The consequences of all serious process failures shall be limited by at least one of the shutdown systems, acting alone, to less than those specified for process system failures, assuming proper action of containment and the emergency core cooling system.

13. The consequences of any serious process system failure accompanied by unavailability of the containment or of the emergency core cooling system shall be limited to less than the specified limits by each of the two shutdown systems acting alone.

14. The essential safety functions (reactor monitoring, reactor shutdown, and decay heat removal) must be shown to be maintained with a high degree of confidence for all accidents starting with any process failure, or any postulated natural or man-made internal or external event. This is in addition to demonstrating conformity with design criteria such as seismic qualification systems and components.